Engineering Ethics

Uma Ferrell

Principal

Ferrell and Associates Consulting, Inc.

Uma@faaconsulting.com

(703)757-9777

Tom Ferrell

Principal

Ferrell and Associates Consulting Inc.

Tom@faaconsulting.com

(703)757-9777

Disclaimer

Opinions expressed in this presentation are those of the presenters, and should not be construed as the opinion of the FAA.

Prologue

The nightly news is full of stories of corporate malfeasance, cheating students, counterfeit drugs, and other ethical lapses that confront us in almost every aspect of our lives. Engineering has not been immune to such problems: witness the unethical decision-making practices that preceded the Space Shuttle Challenger and the removal of important safeguards in the Piper Alpha and Bhopal events. Unfortunately, post event analysis typically shows that missed opportunities for communication and considerable ambiguity (the shades of grey problem) precede the accident. Engineers need a firm grounding in engineering ethics to understand the role they play in highlighting potential safety problems and avoiding unintended detrimental consequences stemming from flawed decision-making. DER decision-making has a fundamental link with engineering ethics – one that is under tremendous pressure in today's 'do more with less environment.'

Understanding the Role We Play

- Aviation safety has evolved over time as the result of lessons learned. Much of that evolution has been focused on very explicit events.
- Software and Complex Electronic Hardware (CEH) are less tangible. To date, we cannot point to any explicit in-service loss of a commercial aircraft due to errant software. We cannot, however, be sure that software has not been a contributing factor in numerous incidents and accidents.
- DO-178B and DO-254 allow for a great deal of latitude in interpretation. The DERs attending this conference, while explicitly only allowed to make findings of compliance, are called upon everyday to answer the question, “what is good enough?”

Is There a Problem?

- Consider the question carefully…
- Examples to Consider:
  - Planning – How much detail? Is it acceptable to simply parrot back ‘DO’ contents?
  - Timing Analysis – what is sufficient? Simple clock counts based on longest execution path; or detailed analysis of cache effects
  - Traceability – To what granularity? To a model or explicit elements within a model? - to the module or to the source line?
  - Robustness Testing – To what level? Acceptable to skip for local variables where ‘controllability and observability’ are difficult or costly to achieve?
- All of these decisions are made in the presence of an applicant who perceives the certification effort to be a major impediment to bringing a product to market as quickly and cheaply as possible.

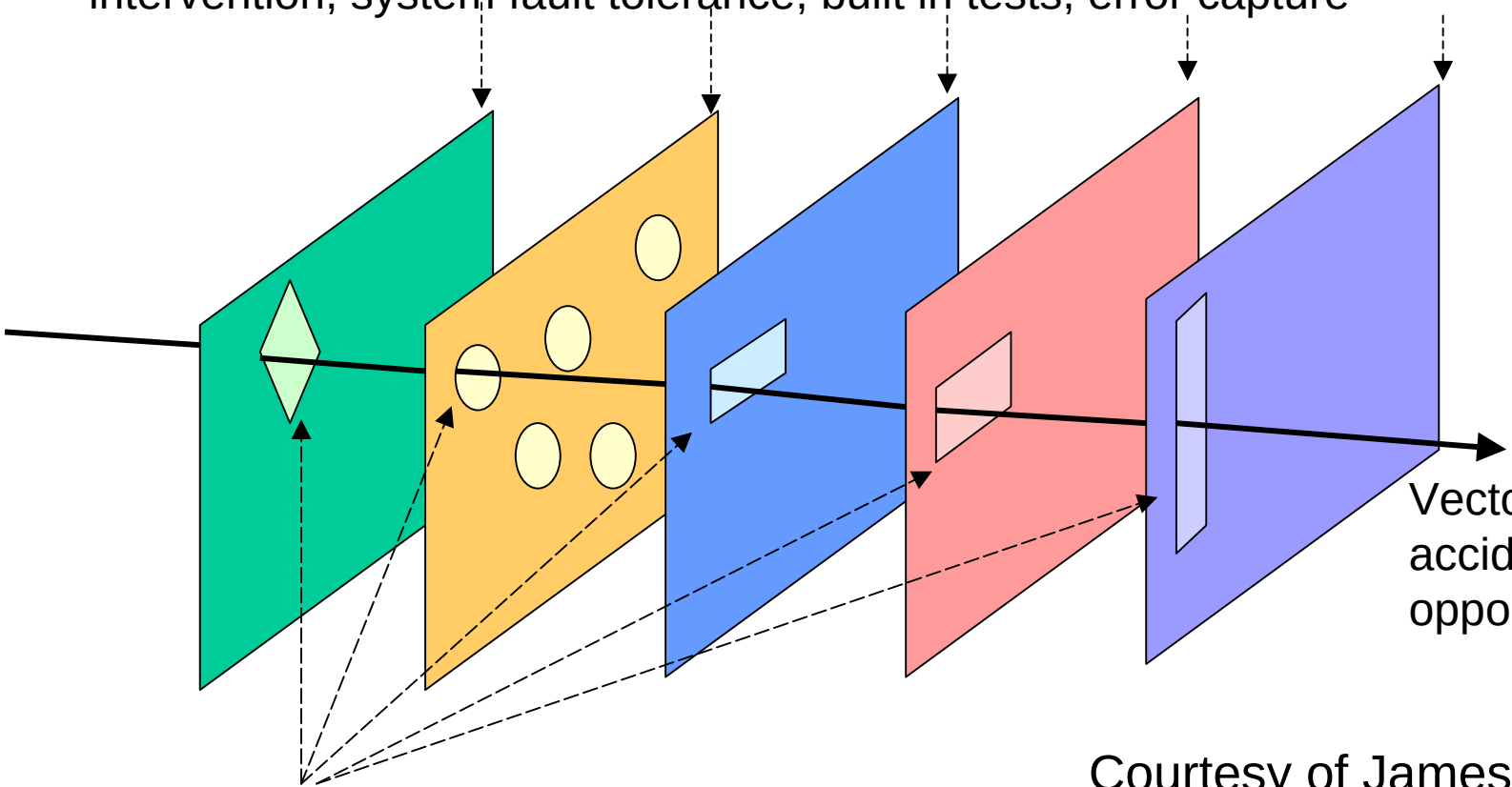
We Think So!

- Industry consolidation, incredibly small profit margins (more often losses) at our end customers, outsourcing of engineering activities, and budget constraints at the FAA are making all of our lives more difficult.
- The pressure to get by with just a little bit less is ever-present and growing. Dr. Richard Feynman characterized the effect as one of “gradually decreasing strictness. The argument that the same risk was flown before without failure is often accepted as an argument for the safety of accepting it again.”
- While some would argue that just the opposite is true – DO-248B, CAST Papers, and so-called ‘generic issue papers’ have accomplished just the opposite, i.e., raised the bar, we are not so sure.

Remember Reason’s Model…

Accident Opportunity Vector

Defensive systems such as design assurance, assurance oversight, operator intervention, system fault tolerance, built in tests, error capture



Courtesy of James Reason

Latent Failures, Local Triggers
Intrinsic Defects, Atypical Conditions

DERs and Engineering Ethics

- If you accept the premise that DERs are one element of an extensive safety net that helps ensure only safe products are fielded, then you must accept that DERs have an ethical responsibility to the general public.
- Consider the following scenarios:
  - Cumbersome or late changes
  - Missing activities or evidence of activities
  - Activities checked as “done” but deemed inadequate
  - Changes in the application of the DO’s due to changes in technology
  - Sliding scale of design assurance activities
  - Previous ‘flawed’ approvals establishing precedent
- As we look at each on of these consider two questions:
  - Who has the burden of proof?
  - What are the shades of grey that the DER is faced with?

Cumbersome or Late Changes

- When safety-related changes to software are cumbersome, some may feel that assuming the risk may be more practical since there may be other safeguards in the system – note that this may occur without properly assessing if these other safeguards are sufficient!
- Late changes following the bulk of the verification activities may introduce additional errors – often with tremendous pressure to minimize regression activities (this is the dead code problem).

Changes to software lead to higher costs, longer schedule, and use of engineers who could be on other profitable programs.

DERs often have to fight for/against such changes, must ensure safety assessment assumptions still hold, and that regression analysis is sufficient.

Missing Activities and Evidence

- In the presence of weak or non-existent SQA, systemic problems and/or lack of data may be present that will require significant rework / reverse engineering.
- DERs are called upon to set the criteria by which the applicant has done enough to make up for previous ‘non-compliances.’
- At what point do you aggregate problems or go for just the big-hitters to maintain the viability of the project?

Missing activities and evidence may be the result of a defined certification strategy – “We’ll just do it this way and then call in a DER at the end – whatever they ask for will be less than if we involve them now.”

Systemic problems are generally not addressable through ‘typical’ SOI audit findings (every single instance). DER must defend the effort being required.

Activities Checked as “Done”

- Coverage analyses in both DO-178B and DO-254 exist to help determine when an applicant has done what is required.
- Unfortunately, requirements traceability and test coverage data are subject to error, and even manipulation.

Assurance activities must be commensurate with the level of software – DERs need to check more samples for higher levels – escalate when problems are found. How do you know you have checked enough?

DERs must recognize that forcing an applicant to do more testing or more detailed structural analysis will likely lead to increased safety margins (through increased confidence in the product) but that such increases simply cannot be measured.

Applying the DO's with New Technology

- If a company has not used a particular technology before, it is new to them!
- DERs should be prepared to go back to first principles with any new technology to ensure the intent of the DO is satisfied, not just the words. Seek FAA guidance for those things truly novel for which no guidance exists.

Assurance activities must be commensurate with the intent of the DO irrespective of technology. DERs MUST stay current with technology to ensure both the type and quantity of design assurance is appropriate.

Understanding the technology and the proper application of design assurance to it should lead to increased safety margins.

The ‘Sliding Scale’

- In addition to the contents of Annex A in both DO-178B and DO-254, DERs recognize that there is some latitude as to exactly how objectives are fulfilled for various assurance levels.
- This ‘sliding scale’ is very helpful in ensuring the focus stays on those portions of the design that have the greatest potential for impacting safety. However, too often the lowest threshold is what the applicant wants applied even when they are working with level A and B devices.

How do you know whether you have followed the intent of DO-178B? Erring on the conservative side may cost the industry a lot more than needed for the level of safety.

DERs should seek FAA guidance if there is any doubt when it comes to what is sufficient. Conservatism here should lead to greater safety margins.

Setting Precedence

- Whatever the reasons, when a certain argument is used for assurance, be mindful of consequences not only for the current project, but also for future projects.
- Applicants often fear such precedents because they feel that it locks them into more work ad infinitum. DERs and FAA Specialists should be similarly concerned that precedents, often euphemistically referred to as IOUs and 'Gentlemen's Agreements,' permanently lower the bar.

Do not assume that the agreement reached on your project will stay confidential. The entire industry may ultimately receive the same treatment that through unintended consequence may lead to lower safety margins overall.

Precedence used for assurance is like software reuse – DERs/FAA must judge whether precedence applies in light of new evidence.

Suggested Solution

- Making the DO's more prescriptive is not the answer. This drives cost, stifles innovation, and, in the end, is unlikely to be effective – new problems will arise. Engineering judgment must be allowed for – it is the underpinning of the designee system.
- FAA Order 8110.37 already lists character as a key trait for the DER, noting that "the [DER] applicant must possess integrity, sound judgment, and a cooperative attitude." Note also that the same order states that "lack of care, judgment, or integrity" is grounds for removal of DER credentials.
- As the pressures increase on the designee community, it seems the time has come for a more formal treatment of the engineering ethics aspect for the work we do.
- Is it time that we introduced code of ethics for DERs?

The Code of Ethics Model

- Virtually every engineering discipline has their own code of ethics. They generally follow a model similar to this blanket statement from the National Institute of Engineering Ethics:

  “Engineers shall hold paramount the health, safety, and welfare of the public in the practice of their profession.”

- DERs responsible for signing for software and CEH owe it to the public, their employer, and to themselves to accomplish all of their work in keeping with the above tenet. If this is too nebulous, consider the more pragmatic model on the next slide.

The Pragmatic Model

When you are faced with making a determination as to whether something is good enough, answer four fundamental questions:

1. Would I be willing to defend my position in a court of law including answering whether what I am accepting represents best practice in industry?
2. Would I be able to stand up to the questioning of a determined ’60 Minutes’ reporter doing an exposé on the latest crash of a commercial airliner?
3. Will I be able to sleep at night after signing for this data?
4. AND – Would I be willing to put my wife/husband, children or parents on an aircraft that is relying on this software or CEH?

Additional References

- http://www.niee.org/ National Institute for Engineering Ethics
- http://onlineethics.org/ The Online Ethics Center for Engineering and Science
- http://www.nspe.org/ethics/eh1-code.asp NSPE code of ethics
- http://www.niee.org/main.htm National Institute for Engineering Ethics
- http://www.ieee.org/portal/site/mainsite/menuitem.818c0c39e85ef176fb2275875bac26c8/index.jsp?&pName=corp_level1&path=about/whatis&file=code.xml&xsl=generic.xsl IEEE code of ethics
- http://www.asce.org/inside/codeofethics.cfm American Society of Civil Engineering code of ethics
- http://www.aiche.org/about/ethicscode.htm American Institute of Chemical Engineers code of ethics
- http://www.asme.org/asme/policies/pdf/p15_7.pdf American Society of Mechanical Engineers code of ethics
- http://www.computer.org/tab/seprof/code.htm#Full IEEE-CS/ACM Software Engineering code of ethics
- http://www.pmi.org/info/AP_MemEthStandards.pdf Project Management Institute code of ethics